UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with DSID 360037038 and email address gillisteam@hotmail.com (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, CA.	)	Case No. 23-950M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 7/24/2023 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Nancy Joseph .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 7/10/2023 @ 11:24 a.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI

Hon. Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with DSID 360037038 and email address gillisteam@hotmail.com (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, CA.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) with Apple reference numbers 202200092013 and 202300155934, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber

Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all instant messages associated with the account from June 1, 2022 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and capability query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My and AirTag logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

f. All records and information regarding locations where the accounts or devices associated with the account were accessed, including all data stored in connection with AirTags Location Services, Find My, and Apple Maps;

g. All records pertaining to the types of service used;

h. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

i. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of 18 U.S.C. §§ 666, 2, and 371, and 18 U.S.C. § 1001, and, since June 1, 2022, including, for each account or identifier listed on Attachment A, information pertaining to the following matters, persons, or entities:

a. Records and information relating to the City of Milwaukee's property;

b. Records and information relating to a conspiracy to defraud the City of Milwaukee;

c. Records and information relating to communications with other City of Milwaukee employees, to include Kyle Hepp and Kelly Behling;

d. Records and information relating to communications with other purchasers or potential purchasers of City of Milwaukee property;

e. Records and information relating to the sale or resale of vehicles and equipment;

f. Records and information relating to the origins or whereabouts of vehicles and equipment offered for sale;

g. Records and information relating to the finances—including but not limited to expenditures, obligations, income, and any financial or monetary transfers—of Kyle Hepp, Kelly Behling, Richard Gillis, and Linda Simcakoski;

h. Records and information relating to the deletion of electronic evidence;

i. Records and information related to possible criminal prosecutions, relevant criminal laws, and investigative methods;

j. The identity of the person(s) who created or used the Apple ID;

k. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

l. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

m. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation, including interests and motivations; and

n. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with DSID 360037038 and email address gillisteam@hotmail.com (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, CA.

Case No. 23-950M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 666, 2, and 371; 18 U.S.C. § 1001	Theft or bribery concerning programs receiving federal funds; conspiracy; false statements

The application is based on these facts:

See attached Affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Eric Burns, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 07/10/2023

Judge's signature

City and state: Milwaukee, WI

Hon. Nancy Joseph, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Eric Burns, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have been a Special Agent with the FBI since November 2009. I am currently assigned to an FBI squad which investigates financial crimes, civil rights crimes, and public corruption crimes. During my tenure with the FBI, I have participated in investigations involving the corruption of public officials, to include facilitation payments and kickbacks. I have participated in all aspects of investigations including executing search warrants involving, among other things, the search and seizure of computers, computer equipment, software, and electronically stored information.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of violations of 18 U.S.C. §§ 666, 2, and 371, and 18 U.S.C. § 1001 (the "SUBJECT OFFENSES"), as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(I)(A), & (c)(I)(A). Specifically, the Court is "a district court of the United States ... that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

The Overall Scheme

6. The FBI is investigating allegations of fraud and abuse by City of Milwaukee ("City"), Department of Public Works ("DPW") employees who conspired to sell City-owned equipment and vehicles to friends and amongst each other at prices significantly below market value, rather than using the City-approved auction house. As further detailed below, these friends in turn posted and sold the City-owned equipment and vehicles on Facebook Marketplace at substantially higher prices than what they purchased them for from the City.

7. On or about August 17, 2020, LONNIE FISCHER was hired as DPW's Fleet Services Manager. On or about April 19, 2021, KYLE HEPP was hired as DPW's Fleet Acquisitions Manager. KELLY BEHLING has worked for the City since April 2014 in various administrative support roles, but most recently served as a DPW Program Assistant in Fleet Services since on or about April 4, 2021. Together, FISCHER, HEPP, and BEHLING were

responsible for, amongst other things, overseeing DPW's equipment disposal process, decommissioning DPW equipment, and preparing/selling surplus DPW equipment.

8. According to an anonymous complaint filed with DPW's Fraud Hotline on September 20, 2022, since being hired as DPW's Fleet Services Manager, FISCHER has been hiring his friends to staff the Fleet Services department, to include hiring HEPP as the Fleet Acquisitions Manager. The anonymous complainant stated HEPP was taking City-owned equipment, ranging from small tools to vehicles, and selling it to his friends, RICK GILLIS and LINDA SIMCAKOSKI, rather than taking the City-owned equipment to auction. According to the anonymous complainant, GILLIS and SIMCAKOSKI then posted and sold the City-owned equipment on Facebook Marketplace at a profit.

9. The anonymous complaint prompted a review of DPW's files, which corroborated many of the details in the complaint. According to information provided by DPW's interim Fleet Services Manager ("INDIVIDUAL-1"), who has been conducting an extensive review of DPW's used equipment sales between January 1, 2020 and September 29, 2022, the City has been defrauded of at least $480,000, due, at least in part, to City-owned equipment and vehicles being sold to individuals at prices significantly below market value rather than using the City-approved auction house to conduct arms-length transactions. INDIVIDUAL-1 has also identified several instances of non-City vehicles being used to remove loads of equipment and surplus items from City facilities. City records revealed GILLIS to be the largest benefactor of City-owned equipment and vehicles being sold to individuals at prices significantly below market value.

10. According to information provided by INDIVIDUAL-1, between June 17, 2022 and September 8, 2022, GILLIS purchased at least 74 items of City-owned equipment or vehicles for approximately $35,130. INDIVIDUAL-1 assessed a fair market value of these items at

approximately $315,850, based on what the City could have received using the City-approved auction house.

Accounts and Contacts

11. According to information received by subpoena from Meta, Facebook account 100002043280466 is registered to email address gillisteam@hotmail.com and subscribed to a "Rick Gillis" (the "Gillis Facebook Account"). The Gillis Facebook Account was created or about January 1, 2011.

12. According to information received by subpoena from Meta on November 7, 2022, Facebook account 1304449376 is registered to email address slippery12no@yahoo.com and is subscribed to a "Linda Simcakoski" (the "Simcakoski Facebook Account"). The Simcakoski Facebook Account was created on or about February 12, 2012.

13. According to information received by subpoena from Sprint, telephone number 262-352-6335 has been subscribed to by GILLIS' spouse since September 13, 2015. GILLIS' spouse is listed as the financially liable party with a billing address of S12W29085 Summit Avenue, Waukesha, WI 53188.

14. According to information received by subpoena from U.S. Cellular, telephone number 262-312-0107 has been subscribed to by HEPP since November 2, 2015. HEPP is listed as the financially liable party with a billing address of 111 Richard Street, Waukesha, WI 53189.

15. According to information received by subpoena from T-Mobile, telephone number 414-210-8076 has been subscribed to by BEHLING since May 29, 2017. BEHLING is listed as the financially liable party with a billing address of 2045 S. 34th St., Milwaukee, WI 53215.

16. According to information received by subpoena from Apple, GILLIS created an iCloud Account on or about September 23, 2014 under the name Richard Gillis (the "Gillis iCloud

Account"). The Gillis iCloud Account is associated with email address gilllisteam@hotmail.com, DSID 360037038, and telephone number 262-652-6335 (the "6335 Phone Number"). The Gillis iCloud Account utilized each of the following services as recently as November 2022: Bookmarks, Calendars, iCloud Photos, Contacts, Find My Friends, iCloud Drive, Messages in iCloud, Notes, and Safari Browsing History. Some of these services are discussed in more detail below. Apple further identified an iPhone as being associated with the Gillis iCloud Account.

17. Between June 14, 2022 and November 8, 2022, according to information received by subpoena, the 6335 Phone Number (GILLIS's) exchanged over a thousand calls and text messages with the telephone number subscribed to by HEPP, including on days and at specific times relevant to the SUBJECT OFFENSES, as further described below.

18. Between June 18, 2022 and September 28, 2022, according to information received by subpoena, the 6335 Phone Number exchanged 20 text messages and 10 telephone calls with the telephone number subscribed to by BEHLING.

Specific Executions of the Scheme

19. A review of the Gillis Facebook Account, received via search warrant, revealed multiple postings for equipment and vehicles for sale that had been "purchased" for far less from the City of Milwaukee. For example, on July 27, 2022, the Gillis Facebook Account listed a 2010 Wain Roy concrete breaker that came off a John Deere 410J for sale at $3,999.

20. On July 26, 2022, according to DPW records, the City recorded the sale of a John Deere 410J for $2,000 to GILLIS[1].

[1] Please note that in other legal process in this matter, your Affiant incorrectly described this specific transaction as the date GILLIS purchased the item from the City. This is more accurately described as the date the City recorded the sale of the item, which may or may not have corresponded with the date GILLIS took possession of the item.

21. On July 26, 2022, according to information received by subpoena, the telephone number subscribed to by HEPP exchanged 32 text messages and one telephone call with the telephone number subscribed to by BEHLING. Additionally, on July 26, 2022, the 6335 Phone Number exchanged seven text messages and two telephone calls with the telephone number subscribed to by HEPP.

22. A review of the Simcakoski Facebook Account, received via search warrant, also revealed multiple postings for equipment and vehicles for sale. For example, in August 2022, the Simcakoski Facebook Account listed a 2004 John Deere 410G Backhoe Loader for sale at $27,999.

23. On August 14, 2022, according to DPW records, the City recorded the sale of a 2004 John Deere 410G for $2,000 to GILLIS[1]. INDIVIDUAL-1 estimated the backhoe's value to be $35,000.

24. On September 28, 2022, according to information received by subpoena from Landmark Credit Union, GILLIS deposited a check into his savings account for $26,500. The memo line on the check stated, "John Deere 410G."

25. With respect to the instances of non-City vehicles being used to remove loads of equipment and surplus items from City facilities, as indicated above, these instances appear to have been coordinated by several DPW employees, to include HEPP and BEHLING, without authorization from the City. For example, surveillance footage of DPW's Central Repair Garage revealed that on Saturday, August 20, 2022, 22 pallets of various materials, six pieces of welding equipment, and a new replacement fuel tank for a City-owned truck, were removed from the secure stockroom and loaded onto a large platform truck and a stake bed truck. DPW's surveillance footage shows HEPP and BEHLING assisting in the removal of these items, and GILLIS present at the scene. INDIVIDUAL-1 assessed a fair market value of these items at approximately

$53,186, based on what the City could have received using the City-approved auction house or, to the extent the items could not be auctioned, recycling the items.

26. According to information provided by INDIVIDUAL-1, DPW has one bill of sale on file to reflect the August 20, 2022 "sale" of the 22 pallets, six pieces of welding equipment, and the new replacement fuel tank for a City-owned truck. The bill of sale indicates three obsolete welders were sold to GILLIS on August 20, 2022 for $150.00.

27. Between August 19, 2022 and August 20, 2022, according to information received by subpoena, the telephone number subscribed to by HEPP exchanged 67 text messages and 11 telephone calls with the telephone number subscribed to by BEHLING. Additionally, between August 19, 2022 and August 20, 2022, the 6335 Phone Number exchanged 11 text messages and 11 telephone calls with the telephone number subscribed to by HEPP.

28. On January 5, 2023, the aforementioned City-owned replacement fuel tank that was removed from DPW's Central Repair Garage on August 20, 2022 was identified as being listed for sale on GILLIS' Facebook Marketplace page. The fuel tank, which cost the City $1,000, was listed for sale for $650.00.

29. On January 7, 2023, an FBI Undercover Employee (UCE-1) sent a message to GILLIS via Facebook Messenger expressing an interest in purchasing the City-owned replacement fuel tank. GILLIS responded that the fuel tank was still available and asked for UCE-1's telephone number.

30. On January 10, 2023, at approximately 5:11pm CST, UCE-1 attempted to place a consensually recorded telephone call to GILLIS at the 6335 Phone Number, which was verified using the FBI's telephonic consensual monitoring system. GILLIS did not answer and UCE-1 did not leave a voicemail.

31. On January 10, 2023, at approximately 5:22pm CST, which is approximately 11 minutes after UCE-1 attempted to place a consensually recorded telephone call to GILLIS at the 6335 Phone Number, according to information received by court order, the telephone number subscribed to by HEPP received one text message from the 6335 Phone Number. Less than a minute later, the telephone number subscribed to by HEPP sent one text message to the 6335 Phone Number.

32. On January 10, 2023, at approximately 7:11pm CST, UCE-1 placed a consensually recorded telephone call to GILLIS at the 6335 Phone Number, which was verified using the FBI's telephonic consensual monitoring system. GILLIS informed UCE-1 that the fuel tank listed for sale was brand new, that it was $650.00, and that GILLIS wanted cash as payment for the fuel tank. UCE-1 and GILLIS agreed to touch base on January 12, 2023 to arrange for a time on January 12, 2023 for UCE-1 to inspect and purchase the fuel tank.

33. On January 12, 2023, UCE-1 and another FBI Undercover Employee (UCE-2) met GILLIS at GILLIS' residence. UCE-1 and UCE-2 were both equipped with audio and video recording software, which I have since listened to and watched. As UCE-1 and UCE-2 drove their vehicle up the driveway of GILLIS' residence, they pointed out several items located on GILLIS' property, to include a Freightliner truck, a trencher, a large trailer bearing the numbers "56733," and a flatbed truck. UCE-1 and UCE-2 proceeded to the front door of GILLIS' residence, where they were greeted by GILLIS. GILLIS walked UCE-1 and UCE-2 to a pole barn located on his property. Located inside the pole barn was the fuel tank UCE-1 and UCE-2 intended to purchase, along with numerous boxes that appeared to be filled with used tools and equipment. The pole barn also contained a large compressor, which UCE-1 inquired about. GILLIS stated it was his father-in-law's, but that he had not run power to it yet because he "[didn't] like getting [his] hands

dirty, I buy and sell shit, that's it." GILLIS also told UCE-1 and UCE-2 that the pole barn where the fuel tank was located "was nothing," and that he had "a warehouse twice this size and it's full of just shit," but that he had "no time to list shit." UCE-2 asked GILLIS if he had anything for their purported landscaping business. GILLIS stated, "I did have lots of stuff, I had grapple buckets, I had grader buckets, I had equipment, I had backhoes, I had tractor backhoes, I was buying all kinds of shit this summer and then everything just kind of went pleh." In discussing used equipment purchasing, GILLIS also said, "municipal equipment's pretty good." He also stated that he had purchased two "Bobcats," used them all summer, and then sold them without losing any money.

34. At the end of the meeting, UCE-2 asked GILLIS if the fuel tank was $650.00 and GILLIS responded, "give me $600.00." UCE-2 handed GILLIS $600.00 in U.S. Currency and UCE-1 and UCE-2 loaded the box containing the fuel tank into their vehicle. GILLIS returned to his residence with the $600.00 in U.S. Currency received from UCE-2.

35. On January 12, 2023, after UCE-1 and UCE-2 transported the box containing the fuel tank to an FBI evidence warehouse, I inspected the box. I observed a torn label on the box, which stated, in part, "STOCKROOM COPY." In reviewing the surveillance footage from the aforementioned August 20, 2022 incident at DPW's Central Repair Garage wherein a new replacement fuel tank for a City-owned truck was removed from the secure stockroom and loaded onto a large platform truck and a stake bed truck, and where GILLIS was present when this occurred, I observed a torn label on the box containing the fuel tank that appears to be identical to the torn label on the box containing the fuel tank UCE-1 and UCE-2 purchased from GILLIS on January 12, 2023.

36. On August 22, 2022, according to DPW records, the City recorded the sale of a 1990 Landa Steam Cleaner 1200 PSI Trailer to GILLIS for $136.36. The City's equipment

identification number for that item is 56733, which is the same number the large trailer exhibited that was located on GILLIS' property when UCE-1 and UCE-2 met GILLIS on January 12, 2023, as indicated above. INDIVIDUAL-1 assessed a fair market value of approximately $1,000 for that item.

Personnel Actions and Prior Investigation

37. According to information provided by DPW, FISCHER, HEPP, and BEHLING were all placed on administrative leave immediately after DPW received the anonymous complaint. FISCHER, HEPP, and BEHLING have all since resigned from DPW in lieu of discharge.

38. On December 21, 2022, HEPP consented to a pre-discharge hearing interview conducted by the City, at which time HEPP was presented with a *Garrity* Warning and *Garrity* Waiver documents. HEPP signed the *Garrity* Waiver. During the interview, HEPP stated that he determined the price of the equipment and vehicles the City sold, to include the equipment and vehicles the City sold to GILLIS, whom he met in 2021. HEPP stated he just looked at the overall condition of the equipment or vehicle and set the price. HEPP stated he understood that he should not have made sales in the manner he did, but blamed FISCHER, stating FISCHER directed this manner of disposal because FISCHER was irritated that DPW had to answer so many questions when selling equipment or vehicles via auction. HEPP denied profiting from the manner in which purchases and sales of City-owned equipment and vehicles were conducted, but indicated he received a benefit because he was able to "use" a vehicle someone he knew purchased from the City. HEPP was also confronted with a picture of a truck he purchased from the City at substantially less than its market value, and subsequently admitted that it was improper to set the value and also purchase the vehicle. With respect to the August 20, 2022 incident at DPW's Central

Repair Garage, HEPP admitted he was present and acknowledged non-City individuals, to include GILLIS, were on site. HEPP claimed that FISCHER told him to get rid of stuff, and was therefore doing what he was doing at the direction of FISCHER.

39. On December 29, 2022, BEHLING consented to a pre-discharge hearing interview conducted by the City, at which time BEHLING was presented with a *Garrity* Warning and *Garrity* Waiver documents. BEHLING signed the *Garrity* Waiver. During the interview, BEHLING re-iterated much of what HEPP said during his pre-discharge hearing interview, but with some minor deviations. According to BEHLING, FISCHER directed the manner of disposal of equipment and vehicles because the process to auction was too cumbersome; however, FISCHER was responsible for deciding which vehicles would be sold to whom and what value they would be assigned. BEHLING stated she also knew GILLIS and that GILLIS bought and subsequently sold the equipment and vehicles he acquired from the City. Like HEPP, BEHLING denied profiting from the manner in which purchases and sales of City-owned equipment and vehicles were conducted, but did admit to purchasing a vehicle from the City for her daughter for $400.00 (INDIVIDUAL-1 estimated the fair market value of the vehicle to be $4,400).

40. On January 4, 2023, prior to a pre-discharge hearing scheduled for FISCHER, FISCHER emailed a Human Resources Representative at DPW requesting DPW allow him to resign from DPW in order to seek other employment prior to the hearing. In that email, FISCHER stated, "I am taking full accountability for all items listed in your email." FISCHER ultimately resigned from DPW prior to the hearing and therefore did not consent to an interview.

41. According to information received via subpoena from Potawatomi Casino, HEPP and BEHLING both frequent the casino. The sums of money they were each gambling increased dramatically during the summer of 2022, when the above-described scheme was at its most active.

Prior Search Warrants

42. On February 13, 2023, law enforcement executed a search warrant of GILLIS's residence and cellular telephone pursuant to a lawful court order dated February 10, 2023. *See* 23-MJ-17. While executing the search warrant, law enforcement also interviewed GILLIS. GILLIS stated, in part, that he was introduced to HEPP by HEPP's brother, who GILLIS worked with. GILLIS stated HEPP's brother turned GILLIS on to purchasing items from DPW. GILLIS further stated that he always purchased items from HEPP and that HEPP told GILLIS that GILLIS had to pay for items in cash. GILLIS also stated that law enforcement was mistaken about what he had paid for vehicles and equipment he purchased from DPW. For example, GILLIS claimed he purchased the 2004 John Deere 410G, as previously discussed in this Affidavit, for $13,000 from the City, not $2,000. GILLIS retrieved receipts he received from the City when he purchased vehicles and equipment, which law enforcement subsequently seized as part of the aforementioned search warrant. GILLIS identified the receipt in question, which law enforcement observed to be nearly identical to the receipt maintained by DPW (but with a different sales price), which indicated GILLIS paid $13,000 for the item. When asked why the receipt maintained by DPW would indicate GILLIS paid a different value for an item than the one GILLIS had in in possession, GILLIS stated he did not know but that he always signed two receipts when he met HEPP at DPW to purchase an item. GILLIS also told law enforcement that after HEPP was placed on Paid Administrative Leave by DPW, HEPP asked GILLIS, on at least two occasions, to get rid of his receipts. GILLIS indicated he was concerned by HEPP's request, and took steps to hide the receipts from HEPP for fear of HEPP destroying them. GILLIS disclaimed any knowledge, however, of HEPP or other City employees personally profiting from GILLIS's purchases of City equipment.

43. A review of the forensic download of GILLIS's cellular device revealed the following:

a. The Apple ID associated with the cellular device was gillisteam@hotmail.com.

b. The cellular device was last restored using an iCloud backup on September 7, 2021.

c. GILLIS conducted several searches on the cellular device using the Google search engine, to include the following notable searches:

i. can i servh for deleted texts

ii. How to retrieve deleted text messages on iPhone 11

iii. lying definition

iv. city of milwaukee employee stealing

v. city of milwaukee admidstration leave

vi. city of milwaukee scandal

vii. city of milwaukee employee scandal

viii. is title skipping illegal

d. The earliest text message between GILLIS and HEPP available on the phone is dated October 16, 2022[2], despite telephone records showing nearly 500 text messages between GILLIS and HEPP since June 2022.

e. A review of the text messages between GILLIS and HEPP that were still contained on the device revealed GILLIS and HEPP primarily discussed having HEPP perform mechanical repairs for GILLIS.

[2] It should be noted that this is referring to text messages between only GILLIS and HEPP. A review of all text messages contained on the device revealed one group text message, dated July 21, 2022, between GILLIS, HEPP, and HEPP's brother. In that group text message, HEPP sent an image of what appears to be a jet flying over a building. GILLIS responded, "Sweet!" HEPP's brother did not respond.

44. On February 18, 2023, law enforcement executed a search warrant of HEPP's cellular telephone pursuant to a lawful court order dated February 9, 2023. *See* 23-MJ-19. While executing the search warrant, law enforcement also interviewed HEPP. During the interview, HEPP was shown the differing receipts for the 2004 John Deere 410G that GILLIS purchased from the City, one receipt indicating it was sold to GILLIS for $2,000 and the other indicating it was sold to GILLIS for $13,000. When questioned about the differing amounts, HEPP stated, in part, that "there was no scheme. There was the thought of making profit, more money, that type of scenario, that's all it was." When asked who HEPP was referring to regarding who made "more money," HEPP stated, "I don't want to incriminate myself whatsoever."

45. A review of the forensic download of HEPP's cellular device revealed the following:

a. The device contained no internet search history prior to January 2, 2023.

b. The earliest text message between HEPP and BEHLING available on the phone is dated November 23, 2022, despite telephone records showing thousands of text messages between HEPP and BEHLING since November 2021.

c. A review of the text messages between HEPP and BEHLING that were still contained on the device revealed HEPP and BEHLING, at times, discussed this investigation. For example, on December 19, 2022, HEPP and BEHLING exchanged screenshots of the letters they separately received from the City regarding their upcoming pre-discharge hearings. Notably, and in response to HEPP receiving a screenshot of BEHLING's pre-discharge hearing letter wherein the City alleged, in part, that BEHLING had "induced, or has attempted to induce, an officer or employee in the service of the city to commit an unlawful act or to act

in violation of any lawful and reasonable departmental or official regulation or order…", HEPP sent BEHLING a screenshot of the definition of "embezzlement."

d. A further review of the text messages between HEPP and BEHLING revealed they likely coordinated their responses to the City in order to blame FISCHER for any misconduct. For example, on December 29, 2022, the day of BEHLING's pre-discharge hearing interview with DPW, HEPP stated "Thinking of you and remember, we did nothing wrong, they will try to say anything they can to pass the blame. We did what we were told by Lonnie." BEHLING responded, "Ik I'm just ready for it to be over. And I still don't see how the hell we get in trouble because of decisions Lonnie made…"

46. On February 22, 2023, law enforcement executed a search warrant of BEHLING's cellular telephone pursuant to a lawful court order dated February 22, 2023. *See* 23-MJ-49. A review of the forensic download of BEHLING's cellular device revealed the following:

a. Similar to HEPP's cellular device, the earliest text message available on the phone between BEHLING and HEPP is dated November 17, 2022, despite telephone records showing thousands of text messages between HEPP and BEHLING since November 2021.

b. The device contained no text messages between BEHLING and GILLIS, despite telephone records showing 20 text messages between BEHLING and the 6335 Phone Number.

Subsequent Interview of GILLIS

47. On February 15, 2023, after reviewing some of the contents on the forensic download of GILLIS's cellular device, I conducted a follow-up interview of GILLIS. GILLIS

stated that he was not sure why all the text messages between him and HEPP would not be on his device. GILLIS stated he sometimes deleted text messages, emails, and other contents on his device because it seemed to help speed up the device. GILLIS further stated that he likely deleted a lot of text messages and emails from his device over the preceding months and years, not just necessarily text messages with HEPP. A review of GILLIS's device, however, reflects that his text messages with other people before October of 2022 were not all deleted.

Interview of HEPP

48. On June 21, 2023, law enforcement interviewed HEPP pursuant to a proffer letter from the United States Attorney's Office for the Eastern District of Wisconsin. HEPP stated that he took over the disposition of DPW equipment and vehicles from BEHLING in or about February or March 2022 and that BEHLING trained him on the disposition process. Shortly after taking over the disposition of DWP equipment and vehicles, FISCHER instructed HEPP and BEHLING to sell a DPW truck via auction, but the auction did not go well. Due in part to the failure to sell the DPW truck via auction, FISCHER told HEPP that he could forego auctioning DPW equipment and vehicles and instead sell DPW equipment and vehicles to employees as a perk to employees. Shortly thereafter, BEHLING approached HEPP and said something to the effect of, "we could make some money here." After considering what BEHLING said, HEPP and BEHLING agreed to skim cash off the top of sales of DPW equipment and vehicles to certain individuals.

49. HEPP stated he knew GILLIS through his brother, who worked with GILLIS, and that he knew GILLIS was generally interested in used vehicles and equipment. After BEHLING told HEPP that they "could make some money here," HEPP reached out to GILLIS to ask GILLIS if he would be interested in purchasing City equipment. GILLIS indicated he was and started frequenting DPW's facilities to purchase equipment. HEPP stated he instructed GILLIS to pay for

DPW equipment and vehicles in cash. To effectuate the scheme, HEPP explained that once a price for a particular item (or items) was agreed upon between HEPP and GILLIS, BEHLING, and sometimes HEPP, printed out two bills of sale in advance of GILLIS arriving at DPW to pay for the item (or items). One bill of sale reflected the negotiated price that HEPP and GILLIS had agreed upon. The other bill of sale reflected a lesser fraudulent price that HEPP and BEHLING gave to give the City. When GILLIS arrived at DPW, both bills of sale were printed out, with the bill of sale reflecting the correct negotiated price on the top and the fraudulent bill of sale on the bottom. Using the correct bill of sale, HEPP covered up everything on the fraudulent bill of sale, with the exception of the signature line. GILLIS signed both copies. HEPP then provided GILLIS with the correct bill of sale for GILLIS's records and quickly turned over the fraudulent bill of sale so that GILLIS would not see it.

50. After the transaction between HEPP and GILLIS was complete and GILLIS had left DPW with the items he purchased, HEPP set aside the amount of cash received from GILLIS equal to the fraudulent bill of sale. HEPP then split the remaining cash received from GILLIS in half, keeping half for himself and giving the remainder to BEHLING. With respect to the amount of cash received from GILLIS equal to the fraudulent bill of sale that HEPP set aside, HEPP took that cash to a store near his house and used the cash to purchase money orders. HEPP then provided the fraudulent bill of sale and the money orders to BEHLING so that she could provide them to the City to deposit. HEPP stated that BEHLING showed him how to do the above process so as to ensure GILLIS did not see that he signed a bill of sale reflecting a different price and to ensure DPW had a signed bill of sale to file with the City. With respect to using cash received from GILLIS equal to the fraudulent bill of sale to purchase money orders, HEPP stated

that BEHLING informed him that money orders were not traceable because individuals were not required to show identification to purchase them.

51. HEPP stated the first time he and BEHLING skimmed cash off the top of a sale of DPW equipment was the first sale to GILLIS. HEPP did not know how much cash, in total, he and BEHLING skimmed off the top of sales to GILLIS, but thought it may have been around $25,000 each. HEPP stated GILLIS did not know what he and BEHLING were doing at the time, but that on one occasion, HEPP believed GILLIS noticed one of the fraudulent bills of sale he signed was different than his (GILLIS's) copy before HEPP had the chance to turn the fraudulent bill of sale over. HEPP recalled GILLIS not caring at the time.

52. After being placed on Administrative Leave by DPW, HEPP stated he deleted stuff off his personal cellular telephone, to include text messages he exchanged with GILLIS. HEPP stated he also changed contact names in his personal cellular telephone, to include the contact names for GILLIS and BEHLING. HEPP further stated that he and BEHLING discussed deleting stuff off their personal cellular telephones and mutually agreed to do so. While HEPP deleted text messages he exchanged with GILLIS, HEPP did not recall any conversations with GILLIS about deleting stuff of their respective cellular telephones.

53. Also after being placed on Administrative Leave by DPW, HEPP stated he informed GILLIS that he (HEPP) was being investigated by the FBI. HEPP recalled going to GILLIS's residence in or about October 2022 and speaking to him in person about the investigation. HEPP stated he told GILLIS everything that he and BEHLING did, to include skimming cash off the top of the items GILLIS purchased from DPW and how GILLIS's bills of sale reflected a different price than what the City had on file. HEPP told GILLIS that GILLIS should get rid of all his bills of sale.

Evidence Likely Possessed by Apple

54. Based on my training and experience, I know that the iCloud is a cloud storage and cloud computing service that Apple provides to its customers and is accessible on their products, including the iPhone. Customers can use the iCloud to backup information, to include SMS and MMS messages, photos, videos, music, calendars, third-party app data, and purchase history from Apple, that is captured and/or stored on their personal mobile devices.

55. Based on a review of information received by subpoena from Apple, the Gillis iCloud Account may have backed up information that may be relevant to this investigation, including iMessages, as well as SMS and MMS messages. For example, the Gillis iCloud Account may contain evidence that the suspects have deleted from their cellular devices in an effort to frustrate this investigation.

56. From my training and experience, I know that Apple customers may use the iCloud to back up their mobile devices, including iPhones, iPads and Macs, as a way to ensure that important information is not lost, as well as a means to save important information that is taking up too much space on their mobile device. It is also a way to ensure that when a mobile device is replaced – either for an upgrade or because a device has been lost, stolen, or damaged, the Apple customer can restore data to the new phone. Relatedly, I understand that items that may have been accidentally or intentionally deleted or otherwise unrecoverable from a device may remain in an iCloud account.

57. There is probable cause to believe that evidence of the SUBJECT OFFENSES will be found in the Target Account because the evidence gathered to date in the investigation suggests that GILLIS has been involved in a public corruption scheme and has an iPhone associated with the Target Account. Based on my training and experience, I know that individuals involved in

criminal schemes often communicate with others, be it victims, conspirators, or unknowing parties, in furtherance of their activities. Here, there is probable cause to believe GILLIS used a cellular telephone number to communicate with others, to include HEPP and BEHLING, and to transmit messages relating to the SUBJECT OFFENSES, which he later deleted from his phone but which may be saved on iCloud. There is therefore probable cause to believe that the Target Account will provide evidence, including, but not limited to, communications between GILLIS and conspirators and/or other unknowing parties.

58. On November 7, 2022, a preservation request under 18 U.S.C. § 2703(f) was sent to Apple regarding Apple accounts registered under email address gillisteam@hotmail.com, requesting Apple preserve available data. On January 31, 2023, a preservation extension request under 18 U.S.C. § 2703(f)(2) was sent to Apple requesting Apple continue to preserve available data.

BACKGROUND CONCERNING APPLE[3]

59. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

60. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

[3] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Manage and use your Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "Introduction to iCloud," available at https://support.apple.com/kb/PH26502; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; and "Apple Platform Security," available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf..

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

61. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

62. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

63. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

64. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to

an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

65. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but may nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

66. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the

files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

67. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

68. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

69. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan

to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

70. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

71. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

72. Based on the forgoing, I request that the Court issue the proposed search warrant.

73. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with DSID 360037038 and email address gillisteam@hotmail.com (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, CA.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) with Apple reference numbers 202200092013 and 202300155934, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber

Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all instant messages associated with the account from June 1, 2022 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and capability query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My and AirTag logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

f. All records and information regarding locations where the accounts or devices associated with the account were accessed, including all data stored in connection with AirTags Location Services, Find My, and Apple Maps;

g. All records pertaining to the types of service used;

h. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

i. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of 18 U.S.C. §§ 666, 2, and 371, and 18 U.S.C. § 1001, and, since June 1, 2022, including, for each account or identifier listed on Attachment A, information pertaining to the following matters, persons, or entities:

a. Records and information relating to the City of Milwaukee's property;

b. Records and information relating to a conspiracy to defraud the City of Milwaukee;

c. Records and information relating to communications with other City of Milwaukee employees, to include Kyle Hepp and Kelly Behling;

d. Records and information relating to communications with other purchasers or potential purchasers of City of Milwaukee property;

e. Records and information relating to the sale or resale of vehicles and equipment;

f. Records and information relating to the origins or whereabouts of vehicles and equipment offered for sale;

g. Records and information relating to the finances—including but not limited to expenditures, obligations, income, and any financial or monetary transfers—of Kyle Hepp, Kelly Behling, Richard Gillis, and Linda Simcakoski;

h. Records and information relating to the deletion of electronic evidence;

i. Records and information related to possible criminal prosecutions, relevant criminal laws, and investigative methods;

j. The identity of the person(s) who created or used the Apple ID;

k. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

l. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

m. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation, including interests and motivations; and

n. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.